Security & Certification Overview

Confidential | August 2025

Prepared for prospective customers and partners of FaiceTech

This document provides a high-level overview of FaiceTech's security posture, certifications, and data handling practices. More detailed documentation, including full audit reports, technical specifications, and compliance evidence packs, is available on request and is shared with customers and qualified prospects only.

1. Introduction

FaiceTech provides real-time facial recognition solutions to help organisations protect their people, premises, and assets. We understand that trusting a technology partner with biometric data is a serious decision, which is why security, compliance, and transparency sit at the centre of everything we do.

This document gives you a clear, plain-English summary of the certifications we hold, how we handle data, and the measures we have in place to keep your information safe.

2. Certifications & Accreditations

We invest heavily in independent verification so you can be confident that our security claims are backed by evidence, not just marketing.

Certification	What It Means
ISO 27001	The international gold standard for information security management. Our ISO 27001 certification means we follow a rigorous, independently audited framework covering risk assessment, access controls, incident management, and continuous improvement.
Cyber Essentials	A UK Government-backed scheme that verifies we have essential technical controls in place to guard against the most common cyber threats, including firewalls, secure configuration, access management, malware protection, and patching.
Cyber Essentials Plus	The enhanced level of Cyber Essentials, which includes hands-on technical testing of our systems by an independent assessor — not just a self-assessment.

ISO 9001	The internationally recognised standard for quality management systems. Our ISO 9001 certification demonstrates that we consistently deliver products and services that meet customer and regulatory requirements, with a focus on continuous improvement and customer satisfaction.
ICO Registered	FaiceTech is registered with the UK Information Commissioner's Office (ICO) as required under the Data Protection Act 2018, confirming we process personal data lawfully and transparently.
Secured by Design (Police CPI)	Awarded by Police Crime Prevention Initiatives (Police CPI), Secured by Design is the official UK police security initiative. This accreditation recognises that our products meet police-preferred standards for crime prevention and physical security.
Surveillance Camera Code of Practice	FaiceTech operates in accordance with the UK Surveillance Camera Code of Practice, which sets out guidelines for the appropriate and proportionate use of surveillance camera systems, including facial recognition. This ensures our solutions are deployed transparently and with respect for individual privacy.
COMING SOON: ISO 42001	ISO 42001 is the international standard for Artificial Intelligence Management Systems. FaiceTech is actively working towards this certification, which will further demonstrate our commitment to the responsible and ethical development, deployment, and use of AI technologies including facial recognition.

3. Data Handling & UK GDPR Compliance

3.1 Data Sovereignty

FaiceTech's primary infrastructure is hosted within the United Kingdom, ensuring that operational data remains under UK legal jurisdiction. Where disaster recovery or resilience measures require it, secondary infrastructure within the EU may be used. No data is processed or stored outside of the UK and EU.

3.2 Biometric Data as Special Category Data

Facial recognition relies on biometric data, which the UK GDPR classifies as "special category" personal data. This means it requires a higher level of protection than standard personal information. FaiceTech applies additional safeguards to biometric data throughout its lifecycle, from capture to deletion, including encryption at rest and in transit, strict role-based access controls, and comprehensive audit logging.

3.3 Independent Algorithm Testing

The facial recognition algorithm used by FaiceTech has been independently evaluated by the National Institute of Standards and Technology (NIST) as part of their Face Recognition Technology Evaluation (FRTE) programme. NIST testing provides an objective, third-party benchmark for algorithm accuracy and demographic fairness.

3.4 Lawful Basis & Data Controller Responsibilities

Under UK GDPR, the organisation deploying FaiceTech's system is typically the Data Controller and is responsible for establishing the lawful basis for processing. Depending on the deployment context, FaiceTech operates as either a Data Processor or a Joint Controller. We provide Data Processing Agreements (DPAs) to every customer, clearly setting out the responsibilities of both parties.

3.5 Data Retention

FaiceTech does not impose a fixed retention period. Instead, data retention is fully customer-controlled. You decide how long alert data and images are retained, in line with your own data protection policies and any relevant legal requirements. When data is no longer needed, it can be securely deleted at any time through the FaiceTech platform.

3.6 Data Protection Impact Assessments (DPIAs)

Because facial recognition involves large-scale processing of biometric data, a DPIA is required before deployment. FaiceTech provides template DPIAs and works with customers to complete them, ensuring all risks are identified, assessed, and mitigated before the system goes live.

4. Sub-Processors

FaiceTech uses a small number of carefully vetted third-party services to support platform operations. All sub-processors are selected and managed using a risk-based approach aligned with GDPR Articles 28 and 32, and are subject to ongoing governance and review under our ISO 27001-certified Information Security Management System (ISMS).

Our primary infrastructure provider is based in the United Kingdom. All sub-processors operate within the UK or EU, and are bound by contractual Data Processing Agreements.

A complete and detailed sub-processor register is available to customers and qualified prospects under NDA. If we add or change a sub-processor, we will notify affected customers in advance and update our Data Processing Agreement.

5. Technical Security Measures

Beyond our certifications, FaiceTech employs a range of practical security measures to protect your data day-to-day:

- **Encryption at Rest & in Transit:** All data is encrypted using industry-standard protocols, including TLS 1.2+ for data in transit. Sensitive fields benefit from additional application-level encryption on top of infrastructure-level controls.
- **Tenant Isolation:** The platform enforces strict tenant isolation at both the application and database level. Each customer's data is completely segregated and cannot be accessed by other organisations.
- **Role-Based Access Control:** Platform access is restricted by role, ensuring users only see the data relevant to their responsibilities.
- **Tamper-Resistant Audit Logging:** Key user and administrative actions are recorded in tamper-resistant audit logs, supporting compliance reporting, governance, and incident investigation.
- **Pseudonymisation & Data Minimisation:** The platform uses system-generated identifiers in place of personal data wherever possible, minimising the exposure of identifiable information within internal systems and logs.
- **Privacy by Design:** Data protection principles are built into the platform architecture from the ground up, including pseudonymisation, configurable retention policies, and auditability as standard.
- **Secure Development Practices:** Our development process follows secure coding standards, with regular code reviews and vulnerability testing.
- **Incident Response:** We have a documented incident response plan that is tested regularly. In the unlikely event of a breach, we will notify affected customers without undue delay as required by UK GDPR.
- **Business Continuity:** Regular backups and disaster recovery procedures are in place to ensure service availability.

6. Data Protection Officer

FaiceTech has a designated Data Protection Officer (DPO) who oversees our compliance with UK GDPR and is available to answer any questions about how we handle personal data.

DPO Contact: dpo@faicetech.com

7. How to Find Out More

We believe in openness. If you have questions about any aspect of our security posture, certifications, or data handling practices, we are happy to provide additional detail. Please don't hesitate to get in touch.

FaiceTech

Website: faicetech.com

Email: info@faicetech.com

DPO: dpo@faicetech.com